

# A Family of Translations for Pseudo-Boolean Constraints to CNF

Amir Aavani<sup>1</sup>, David Mitchell<sup>1</sup>, and Eugenia Ternovska<sup>1</sup>

Simon Fraser University, Computing Science Department  
`{aaa78,mitchell,ter}@sfu.ca`

**Abstract.** A Pseudo-Boolean constraint, PB-constraint, is a linear constraint over Boolean variables. This kind of constraints has been widely used in expressing NP-complete problems.

This paper introduces a family of algorithms for translating Pseudo-Boolean constraints into CNF clauses. These algorithms are centered around the idea of rewriting a PB-constraint as the conjunction of a set of easier to translate constraints, we call them PBMod-constraints. The CNF produced by the proposed encoding has small size, and we also characterize the constraints for which one can expect the SAT solvers to perform well on the produced CNF. We show that there are many constraints for which the proposed encoding has a good performance.

We compared the running time of SAT solvers on the output of the proposed translation and the existing approaches.

## 1 Introduction

A Pseudo-Boolean constraint (PB-constraint), which is also known as 0-1 integer linear constraint by the integer linear programming community, is a generalization of a clause. A PB-constraint is an inequality (equality) on a linear combination of Boolean literals:

$$\sum_{i=1}^n a_i l_i \{<, \leq, =, \geq, >\} b,$$

where  $a_1, \dots, a_n$  and  $b$  are constant integers and  $l_1, \dots, l_n$  are literals. The left-hand side of a PB-constraint under assignment  $\mathcal{A}$  is equal to the sum of the coefficients whose corresponding literals are mapped to *true* by  $\mathcal{A}$ .

One way to build a solver which is capable of handling PB-constraints is to modify a SAT solver to support PB-constraints natively. PBS [3] and PUEBLO [12] are examples of such solvers. The main challenge in this approach is to modify/extend all the heuristic functions used in the original SAT solver. Another approach is to replace a given PB-constraint with a logically equivalent set of clauses and then use a SAT solver to find a solution. The main benefit of the latter approach is that every SAT solver, even those which are going to be developed in future, can be plugged in to the system. Also, there are certain NP problems which can be translated into a combination of a relatively small CNF formula plus one or two PB-constraints. One can name Vehicle Routing Problem

and its variations [10], Hamiltonian Cycle problem and Knapsack as examples of such problems. Having a *good* translation for PB-constraints enables both naive and expert users to use SAT solvers for attacking these problems. Most professional users encode these problems using Integer Linear Programming (ILP) tools. Unfortunately, there is no natural way to express certain sentences in an integer linear program, e.g. “Either John or Maria is wearing a green shirt and a black hat”.

We define a PMod-constraint to be:

$$\sum_{i=1}^n a_i l_i \equiv b \pmod{M},$$

where  $a_1, \dots, a_n$  and  $b$  are non-negative integers less than  $M$ , and  $l_1, \dots, l_n$  are literals.

In Section 3, we show that instead of translating a given PB-constraint, we can translate a set of appropriately selected PMod-constraints. So to translate PB-constraints to SAT, we need to determine how to *choose* the set of PMod-constraints and how to *translate* a PMod-constraint to SAT. As we show in this paper, there are many PB-constraints whose unsatisfiability can be proven by showing the unsatisfiability of a PMod-constraint. Some of our translations for PMod-constraints allow unit-propagation to infer inconsistency if the current assignment cannot be extended to a satisfying assignment for that PMod-constraint and hence unit-propagation can infer inconsistency for the original PB-constraint. In Section 6, it has been shown that the number of PB-constraints for which unit-propagation can infer inconsistency, given the output of proposed translations, is much larger than the other existing encodings. Also, we prove that it is impossible to translate all PB-constraints in the form  $\sum a_i l_i = b$  into polynomial size arc-consistent CNF unless  $P=CoNP$ .

The structure of this paper is as follows: The next section is devoted to preliminaries and definitions. The proposed encoding is presented in Section 3 and 4. In Section 5, four existing translations (encodings) for converting a PB-constraint to CNF are described. In Section 6, we study the performance of unit propagation on the resulting CNF of different encodings. Specifically, we describe a necessary condition on the instances for which our translation is arc-consistent, and also show that there is no polynomial size arc-consistent encoding for PB-constraint in the form  $\sum a_i l_i = b$  unless  $P=CoNP$ .

## 2 Background

In this section, we fix our notations and use them through the rest of this paper. Also, we define when an encoding produces a *valid translation*.

### 2.1 Notations

Let  $X$  be a set of Boolean variables. A literal,  $l$ , is either a Boolean variable or negation of a Boolean variable and  $var(l)$  denotes the variable corresponding to  $l$ . A clause on  $X$ ,  $C = \{l_1, \dots, l_m\}$ , is a set of literals such that  $var(l_i) \in X$ . An

assignment  $\mathcal{A}$  to  $X$  is a function that maps some variables in  $X$  to either *true* or *false*. By  $x \in \mathcal{A}^+ (x \in \mathcal{A}^-)$  we mean that *true* (*false*) is assigned to  $x$  under assignment  $\mathcal{A}$ . Also, we use  $\mathcal{A} [S]$ ,  $S \subseteq X$ , as a shorthand for the assignment obtained by restricting the domain of  $\mathcal{A}$  to the variables in  $S$ .

PB-constraint  $Q$  on  $X$  is specified as:

$$a_1 l_1 + \dots + a_n l_n \quad \{<, \leq, =, \geq, >\} \quad b,$$

where each  $a_i$  is the integer *coefficient* of  $l_i$ ;  $b$  is an integer, called *bound*, and  $l_i$  is a literal, s.t.,  $\text{var}(l_i) \in X$ .

Assignment  $\mathcal{A}$  to  $X$  is a *total assignment* if it assigns a value to each variable in  $X$ , i.e.,  $\mathcal{A}^+ \cup \mathcal{A}^- = X$ . Assignment  $\mathcal{A}$  satisfies literal  $l$ ,  $\mathcal{A} \models l$ , if  $l = x$  and  $x \in \mathcal{A}^+$  or  $l = \neg x$  and  $x \in \mathcal{A}^-$ . Assignment  $\mathcal{A}$  satisfies clause  $C = \{l_1, \dots, l_m\}$  if there exists at least one literal  $l_i$  such that  $\mathcal{A} \models l_i$ . A total assignment falsifies clause  $C$  if it does not satisfy any of its literals. An assignment satisfies a set of clauses if it satisfies all the clauses in that set. Total assignment  $\mathcal{A}$  to  $X$  satisfies a PB-constraint  $Q$  on  $X$ ,  $\mathcal{A} \models Q$ , if the value of left-hand side of  $Q$  under  $\mathcal{A}$ , i.e.,  $\sum_{i: \mathcal{A} \models l_i} a_i$  and that of right-hand side of  $Q$  satisfies the comparison operator.

We say assignment  $\mathcal{A}$  extends assignment  $\mathcal{B}$ ,  $\mathcal{A} \supseteq \mathcal{B}$ , iff both  $\mathcal{B}^+ \subseteq \mathcal{A}^+$  and  $\mathcal{B}^- \subseteq \mathcal{A}^-$  hold.

## 2.2 Valid Translation

Here, we formalize the meaning of translation of a constraint into CNF and we use this definition to prove the correctness.

Note that a constraint can be seen as a Boolean function which returns *true* on assignments that satisfy the constraint and *false* otherwise.

**Definition 1** Given Boolean function  $F(X)$ , where  $X = \{x_1, \dots, x_n\}$  is a set variables, we call the pair  $\langle v, C \rangle$ , where  $v$  is a Boolean variable,  $C = \{C_1, \dots, C_m\}$  is a set of clauses on  $X \cup Y \cup \{v\}$  and  $Y$  is a set of (auxiliary) propositional variables, a valid translation if  $C$  is satisfiable and for every total assignment  $\mathcal{A}$  to  $X \cup Y \cup \{v\}$  that satisfies  $C$ ,  $\mathcal{A}$  satisfies  $F(X)$  iff it maps  $v$  to true, i.e.,  $C \not\models \perp$ , and:

$$C, \mathcal{A}[X] \models v \Leftrightarrow F(X|_{\mathcal{A}}) = \text{true}.$$

Intuitively,  $C$  describes the relation among input variables,  $x \in X$ , auxiliary variables,  $y \in Y$ , and  $v$ . The truth value of  $v$  is the same as the truth value of  $F(X)$  under all assignments which satisfy  $C$ .

**Observation 1** Let  $Y = F(X)$  be an  $n$ -input  $m$ -output Boolean function. Function  $F$  can be described using  $m$  Boolean functions  $(f_1(X), \dots, f_m(X))$  where  $f_i$  computes the  $i$ -th output of  $F$ . Then a valid translation for  $F$  can be constructed using valid translations for  $f_i$ 's. Let  $\langle v_i, C_i \rangle$  be valid translation for  $f_i$ , for  $i = 1 \dots m$ . Pair  $\langle V, C \rangle$  is a valid translation for  $F$ , where  $V = \{v_1, \dots, v_m\}$  and  $C = \cup C_i$ .

In [5], a translation is defined to be just a set of clauses. It is easy to verify that these two definitions are equivalent.

It worths mentioning that our definition of a valid translation is not limited to PB-constraints.

**Example 1** Let  $Q$  be the following PB-constraint which is not satisfiable. Based on definition 1, the pair  $\langle v, \{C_1\} \rangle$  where  $C_1 = \{\neg v\}$  is a valid translation for  $Q$ .

$$Q : 2x_1 + 4\neg x_2 = 3.$$

### 2.3 Tseitin Transformation

The usual method for transforming a propositional formula to CNF is by the method of Tseitin[14]. In this transformation, a fresh propositional variable is created to represent the truth value of each subformula of the given formula. Let  $\psi_1, \psi_2, \psi$  be three such subformulas and  $x, y, z$  be the associated propositional variables to  $\psi_1, \psi_2$  and  $\psi$ , respectively. The transformation works as follows:

1.  $\psi = \psi_1 \vee \psi_2$  : produce the following three clauses  $\{\neg z, x, y\}, \{z, \neg x\}, \{z, \neg y\}$ :  
(i.e.,  $z \Leftrightarrow x \vee y$ ),
2.  $\psi = \psi_1 \wedge \psi_2$  : produce the following three clauses  $\{\neg z, x\}, \{\neg z, y\}, \{z, \neg x, \neg y\}$ :  
(i.e.,  $z \Leftrightarrow x \wedge y$ ),
3.  $\psi = \neg \psi_1$  : produce the following two clauses  $\{\neg z, \neg x\}, \{z, x\}$  (i.e.,  $z \Leftrightarrow \neg x$ ),
4.  $\psi = v$ , where  $v$  is a propositional variable: produce the following two clauses  $\{\neg z, v\}, \{z, \neg v\}$  (i.e.,  $z \Leftrightarrow v$ ).

### 2.4 Canonical Form

Let consider the following PB-constraint:

$$a_1 l_1 + \dots + a_n l_n = b, \tag{1}$$

where all constant integers ( $a_1 \dots a_n$  and  $b$ ) are positive integers. We show that every PB-constraint can be rewritten as a PB-constraint in form of 1.

**Definition 2** Constraints  $Q_1$  on  $X$  and  $Q_2$  on  $Y \supseteq X$  are equivalent iff for every satisfying assignment  $\mathcal{A}$  for  $Q_1$ , there exists at least one expansion of  $\mathcal{A}$  to  $Y$  satisfying  $Q_2$ , and for every total assignments  $\mathcal{A}$  to  $X$  which does not satisfy  $Q_1$ , all possible expansions of  $\mathcal{A}$  to  $Y$  falsifies  $Q_2$ .

**Observation 2** Let  $n \geq 1$ . The following PB-constraints are equivalent.

1.  $\sum_{i=1}^n a_i l_i \geq b$ ,
2.  $\sum_{i=1}^n a_i l_i > b - 1$ ,
3.  $\sum_{i=1}^n -a_i l_i \leq -b$ ,
4.  $\sum_{i=1}^n -a_i l_i < 1 - b$ .

**Observation 3** Let  $m$  and  $n$  be such that  $1 \leq m \leq n$ . Then (1) and (2) are equivalent.

1.  $\sum_{i=1}^{m-1} a_i l_i + a_m l_m + \sum_{i=m+1}^n a_i l_i < b$ ,
2.  $\sum_{i=1}^{m-1} a_i l_i - a_m \neg l_m + \sum_{i=m+1}^n a_i l_i < b - a_m$ .

Observation 2 and observation 3 imply that every PB-constraint whose comparison operator is in  $\{\leq, <, >, \geq\}$  can be rewritten as an equivalent PB-constraint with positive coefficients in the following form:

$$\sum_{i=1}^n a_i l_i < b. \quad (2)$$

If the right-hand side of (2),  $b$ , is less than or equal to zero, no assignment satisfies the constraint, i.e., the pair  $\langle v, \{\{\neg v\}\} \rangle$  can be used a valid translation for it. It is not hard to observe that if we have a PB-constraint whose left-hand side is 1, pair  $\langle v, \{\{\neg v, \neg l_1\}, \dots, \{\neg v, \neg l_n\}, \{v, l_1, \dots, l_n\}\} \rangle^1$  is a valid translation for that constraint.

**Proposition 1** *Let  $n \geq 1$ ,  $a_i \geq 0, b > 1$  and  $B = \lfloor \log_2 b \rfloor$ . Also, assume the variables  $y_i$  are newly introduced Boolean variables. Then (1) and (2) are equivalent.*

1.  $\sum_{i=1}^n a_i l_i < b$
2.  $\sum_{i=1}^n a_i l_i + \sum_{i=0}^B 2^i y_i = b - 1$

In conclusion, every PB-constraints can be rewritten as an equivalent normalized PB-constraint in form 1. So, if we know how to find a valid translation for a PB-constraint in form (1), we can find a valid translation for every PB-constraint, as well.

## 2.5 Unit Propagation

*Unit propagation* (UP) is a mechanism used by SAT solvers to accelerate the search process. Whenever the current partial assignment maps all but one of the literals in a clause to false, the value of the remaining literal should be true if the instance is satisfiable. A similar situation can happen for PB-constraints, i.e., given a partial assignment  $\mathcal{A}$  and a PB-constraint  $Q$  on  $X$ , there might be a variable that takes the same value in all satisfying expansion of  $\mathcal{A}$ . So, the value for that variable is forced.

Given an assignment  $\mathcal{A}$ , the PB-constraint  $Q$  on  $X$  can be transformed to an equivalent PB-constraint  $Q'$  on  $Y$  such that all the variables in  $Y$  are unassigned under  $\mathcal{A}$ :

$$Q : \sum a_i l_i = b$$

$$Q' : 0 + \sum_{i: \text{var}(l_i) \in Y} a_i l_i = b - \sum_{i: \mathcal{A} \models l_i} a_i$$

---

<sup>1</sup> The clauses in  $C$  corresponds to  $v \Leftrightarrow \neg l_1 \wedge \dots \neg l_n$ .

The terminology used here is an adaptation of what has been used in [5]. A translation for the given constraint  $Q$  is *UP-detectable* if UP infers inconsistency whenever there is no assignment that satisfies  $Q$ . A translation for the given constraint  $Q$  is *UP-inferable* if, for any literal  $l$ , UP infers the value of  $l$  whenever  $l$  takes the same value in all satisfying solutions to  $Q$ . More formally, let  $\langle v, C \rangle$  be a valid-translation for  $Q$  on  $X$ . The pair  $\langle v, C \rangle$  is UP-detectable if  $Q \models \perp \Leftrightarrow C \wedge v \vdash_{UP} \perp$ . It is UP-inferable if  $Q \models l \Leftrightarrow C \wedge v \vdash_{UP} l$ . A translation for  $Q$  is *generalized arc-consistent*, or simply arc-consistent, if it is both UP-detectable and UP-inferable. An encoding is arc-consistent if it produces an arc-consistent translation for all possible input constraints.

### 3 Proposed Method

In this section, we focus on describing how our proposed approach works on the PB-constraints which are in the following form:

$$\sum_{i=1}^n a_i x_i = b, \quad (3)$$

where all constants are positive integers and  $x_i \neq x_j$ , for all  $i \neq j$ .

Let a normal PMod-constraint be an equation in the following form:

$$\sum_{i=1}^n a_i x_i \equiv b \pmod{M}, \quad (4)$$

where  $0 \leq a_i < M$  for all  $1 \leq i \leq n$  and  $0 \leq b < M$ . Total Assignment  $\mathcal{A}$  is a solution to a PMod-constraint iff the value of left-hand side summation under  $\mathcal{A}$  minus the value of right-hand side of the equation,  $b$ , is a multiple of  $M$ .

**Definition 3** *PMod-constraint  $Q[M] : \sum a'_i x_i \equiv b' \pmod{M}$  is called to be the conversion of PB-constraint  $Q : \sum a_i x_i = b$ , modulo  $M$  iff:*

1.  $a'_i = a_i \pmod{M}$ ,
2.  $b' = b \pmod{M}$ .

One can verify that each solution to PB-constraint  $Q$  is also a solution to all its conversions module  $M$ ,  $Q[M]$ ,  $M \geq 2$ . Also, for appropriately large values of  $M$ , each solution to  $Q[M]$  is a solution to  $Q$ . So, for the appropriate values of  $M$ , the two constraints have the same set of solutions. Our goal is to select the value of  $M$  such that translating the corresponding PMod-constraint is easier than translating the original PB-constraint.

**Lemma 1** *For any PB-constraint  $Q : \sum a_i x_i = b$ , if  $M$  satisfies  $M > S = \sum a_i$ , PMod-constraint  $Q[M]$  and PB-constraint  $Q$  have exactly the same set of solutions, i.e., any assignment either satisfies both equations or neither of them.*

**Proof** It is obvious that if  $\mathcal{A}$  is a solution for  $Q$ ,  $\mathcal{A}$  satisfies  $Q[M]$ , too. Now, let's  $\mathcal{A}$  be a solution (a satisfying assignment) for  $Q[M]$ . The value of left-hand side of  $Q[M]$  under  $\mathcal{A}$  should be an integer in the form  $b + k * M$  for some  $k \geq 0$ . As we have  $0 \leq b + k * M \leq \sum a_i < M$ , we can infer that  $k$  should be zero and so the sum of left-hand side of  $Q[M]$  under  $\mathcal{A}$  is exactly equal to  $b$ .

**Lemma 2** *Let  $Q : \sum a_i x_i = b$  be a PB-constraint. Also, let  $M_1$  and  $M_2$  be two integers and  $M_3 = \text{lcm}(M_1, M_2)$ . Assume  $S_j$  is the set of assignments satisfying  $Q[M]$  when  $M = M_j$ , for  $j = 1, 2$  and  $3$ . We have:*

$$S_3 = S_1 \cap S_2.$$

**Proof** The proof of this Lemma is very similar to the proof of the following statement (which can be found in any number theory book, as an exercise): Let  $M_1, M_2$  and  $M_3$  be three integers s.t.  $M_3 = \text{lcm}(M_1, M_2)$ . Then for any integer  $x$  and  $y$  we have:

$$x \equiv y \pmod{M_1} \wedge x \equiv y \pmod{M_2} \Leftrightarrow x \equiv y \pmod{M_3}.$$

Lemma 2 tells us that in order to find the set of answers to a PMod-constraint modulo  $M_3 = \text{lcm}(M_1, M_2)$ , one can find the set of answers to two PMod-constraints (modulo  $M_1$  and  $M_2$ ) and return their intersection.

**Proposition 2** *Let  $\mathbf{M} = \{M_1, \dots, M_m\}$  be a set of  $m$  positive integers. The set of assignments satisfying  $Q : \sum a_i x_i = b$  is exactly the same as the set of assignments satisfying all the  $m$  PMod-constraints,  $Q[M_1], Q[M_2], \dots, Q[M_m]$  if  $\text{lcm}(M_1, \dots, M_m) > S = \sum a_i$ .*

**Theorem 1** *Let  $Q : \sum a_i x_i = b$  be a PB-constraint. Assume we have access to a translation oracle which produces a valid translation for every PMod-constraint. Let  $\mathbf{M} = \{M_1, \dots, M_m\}$  be as described in Prop. 2, and the pair  $\langle v_k, C_k \rangle$  be a valid translation for  $Q[M_k]$  obtained using the translation oracle. Then, pair  $\langle v, C \rangle$ , where  $C = \cup_k C_k \cup C'$  and  $C'$  is the set of clauses describing  $v \Leftrightarrow (v_1 \wedge v_2 \dots \wedge v_m)$ , is a valid translation  $Q$ .*

Theorem 1 can be proved by a straightforward application of Lemma 1 and Proposition 2.

We know  $\text{lcm}(2, \dots, k) \geq 2^{k-1}$ , [8], so set  $\mathbf{M}^N = \{2, \dots, \lceil \log \sum a_i \rceil + 1\}$  can be used as the set of modulus for encoding  $Q : \sum a_i x_i = b$ .

Another candidate for set  $\mathbf{M}$  is subset of prime numbers. One can enumerate the prime numbers and add them to the set of modulus,  $\mathbf{M}^P$ , until their multiplication exceeds  $S$ , i.e., to select  $\mathbf{M}^P$  to be  $\{2, 3, \dots, P_m\}$ . The next proposition gives us an estimation for the size of set  $\mathbf{M}^P$  as well as the maximum value in  $\mathbf{M}^P$ .

**Proposition 3** *Let  $\mathbf{M}^P$  be the set of primes less than or equal to  $P_m$  (assume  $P_m$ , itself, is a prime number) such that*

$$\prod_{p \in \mathbf{M}^P} p \geq S.$$

*Then:*

1.  $m = |\mathbb{M}^P| = \theta(\frac{\ln S}{\ln \ln S})$ .
2.  $P_m < \ln S$ .

Proof of this proposition can be found in the appendix A.

The number of modulus, i.e., the size of  $\mathbb{M}$ , can be reduced if we choose larger modulus. One way to do so is to select the set of modulus to be  $\mathbb{M}^{PP} = \{P_i^{n_i} : P_i \text{ is } i\text{-th prime number and } P_i^{n_i-1} \leq \log S \leq P_i^{n_i}\}$ . So, we have fewer modulus while each modulus is not too big.

**Proposition 4** *Let  $\mathbb{M}^{PP} = \{P_i^{n_i} : P_i \text{ is } i\text{-th prime number and } P_i^{n_i-1} \leq \ln S \leq P_i^{n_i}\}$  be such that*

$$\prod_{M \in \mathbb{M}^{PP}} M \geq S.$$

*Then:*

1.  $m = |\mathbb{M}^{PP}| \leq \frac{\ln S}{\ln \ln S}$ ,
2.  $\max_{M \in \mathbb{M}^{PP}} M = \ln S$ .

**Proof**

1.  $S \leq \prod_{M \in \mathbb{M}^{PP}} M \leq (\ln S)^m \Rightarrow \frac{\ln S}{\ln \ln S} \leq m$ .
2. it comes from the construction of  $\mathbb{M}^{PP}$ .

Note that  $\mathbb{M}^N$ ,  $\mathbb{M}^P$  and  $\mathbb{M}^{PP}$  are just three possible sets of modulus. Given PB-constraint  $Q$ , there are many other candidates for the set of modulus.

It is worth mentioning that the size of description of PB-constraint  $Q : \sum a_i x_i = b$  is  $\theta(n \log a_{Max})$  where  $n$  is the number of literals (coefficients) in the constraint and  $a_{Max}$  is the maximum value of coefficients. The size of description of PMod-constraint  $Q[M]$  is  $\theta(n \log M)$  where  $n$  is the number of literals (coefficients) in the constraint. So, if we can come up with a translation for  $Q[M]$  which produces a CNF with  $O(n^{k_1} M^{k_2})$ , for some constants  $k_1$  and  $k_2$ , clauses/variables (which is exponential in its input size), we have translated the PB-constraints into CNF using a polynomial number of variables (clauses, literals) with respect to the size of representation of the original PB-constraint. Several such translations are described in the next section.

## 4 Encoding For Modular Pseudo-Boolean Constraints

In this section, we describe how a PMod-constraint in the format of Equation (5), where  $0 \leq a_i, b < M$ , can be translated into CNF. Remember that our ultimate goal is not to translate PMod-constraints but to translate PB-constraints.

$$\sum_{i=1}^n a_i l_i = b \pmod{M}. \quad (5)$$

#### 4.1 Translation Using DP

The translation presented here encodes PBMod-constraints using a Dynamic Programming approach. Auxiliary variable  $D_m^l$  is defined inductively as follows:

$$D_m^l = \begin{cases} \top & l \text{ and } m \text{ are both zero;} \\ \perp & l = 0 \text{ and } m > 0; \\ (D_{(m-a_l) \bmod M}^{l-1} \wedge x_l) \vee (D_m^{l-1} \wedge \neg x_l) & \text{Otherwise.} \end{cases}$$

This encoding is similar to translation through BDD, described in [7]. Using a top-down approach, starting from  $D_b^n$ , for describing the Tseitin variables usually generates a smaller CNF.

In this encoding, auxiliary variable  $D_m^l$  describes the necessary and sufficient condition for satisfiability of subproblem  $\sum_{i=1}^l a_i x_i \equiv m \pmod{M}$ .

**Proposition 5** *Let  $D = \{D_m^l\}$  and  $C$  be the clauses which are used to describe the variables in  $D$ . Then, the pair  $\langle D_b^n, C \rangle$  is valid translation for (5).*

Adding the following clauses helps unit propagation to infer more facts:

1. For each  $l, m_1, m_2$ , where  $m_1 \leq m_2$ :  $\{\neg D_{m_1}^l, \neg D_{m_2}^l\}$ . This clause asserts that  $\sum_{i=1}^l a_i x_i$ , modulo  $M$ , cannot be evaluated as both  $m_1$  and  $m_2$ .
2. For each  $l$ :  $\{D_m^l | m = 0 \cdots M-1\}$ . This clause asserts that  $\sum_{i=1}^l a_i x_i$ , modulo  $M$ , is among  $0, 1, \dots, M-1$ .

**Proposition 6** *We can use the following set of clauses to describe the relation among  $D_m^l, D_{m-a_l}^{l-1}, D_m^l, x_l$ :*

1. If both  $D_{m-a_l}^{l-1}$  and  $x_l$  are True, we should have  $D_m^l$  is True, i.e.,  $\{\neg D_{m-a_l}^{l-1}, \neg x_l, D_m^l\}$ ;
2. If  $D_m^{l-1}$  is True and  $x_l$  is False, we should have  $D_m^l$  is True, i.e.,  $\{\neg D_m^{l-1}, x_l, D_m^l\}$ ;
3. If both  $D_m^l$  and  $x_l$  are True, we should have  $D_{m-a_l}^{l-1}$  is True, i.e.,  $\{\neg D_m^l, \neg x_l, D_{m-a_l}^{l-1}\}$ ;
4. If  $D_m^l$  is True and  $x_l$  is False, we should have  $D_m^{l-1}$  is True, i.e.,  $\{\neg D_m^l, x_l, D_m^{l-1}\}$ ;
5. At most one of  $D_0^l, \dots, D_{M-1}^l$  can be True:  $\{\neg D_i^l, \neg D_j^l\}$  ( $0 \leq i < j < M$ );
6. At least one of  $D_0^l, \dots, D_{M-1}^l$  is True:  $\{D_0^l, D_1^l, \dots, D_{M-1}^l\}$ ;

Using this set of clauses results in an encoding for PBMod-constraints with the following property:

Given partial assignment  $\mathcal{A}$ , if there is no total assignment satisfying  $C$  and extending  $\mathcal{A}$  which maps  $\sum_{i=1}^a a_i x_i$  to  $m$ , then unit propagation infers false as the value for variable  $D_a^m$ .

#### 4.2 Translation Using DC

The translation presented here resembles a Divide and Conquer approach. Variable  $D_a^{s,l}$  is defined inductively as follows:

$$D_m^{s,l} = \begin{cases} \top & m \text{ and } l \text{ are both zero;} \\ \perp & l = 0 \text{ and } m \neq 0; \\ x_s & l = 1 \text{ and } m \neq 0 \text{ and } a_s = m; \\ \neg x_s & l = 1 \text{ and } m = 0 \text{ and } a_s \neq 0; \\ \perp & l = 1 \text{ and } m \neq 0 \text{ and } a_s \neq m; \\ \top & l = 1 \text{ and } m = a_s = 0; \\ \bigvee_{a'=0}^{M-1} (D_{(m-a' \bmod M)}^{s,l/2} \wedge D_{a'}^{s+l/2,l/2}) & \text{Otherwise.} \end{cases}$$

Here,  $D_a^{s,l}$  describes the necessary and sufficient condition for satisfiability of subproblem  $\sum_{i=s}^{s+l-1} a_i x_i \equiv a \pmod{M}$ .

**Proposition 7** *Let  $D = \{D_a^{s,l}\}$  and  $C$  be the clauses which are used to describe the variables in  $D$ . Then, pair  $\langle D_b^n, C \rangle$  is a valid translation for (5).*

Similar to translating using DP, by adding the following clauses, we can boost the performance of unit propagation for this translation, too.

1. For each  $s, l, m_1, m_2$ , where  $m_1 \leq m_2$ :  $\{\neg D_{m_1}^{s,l}, \neg D_{m_2}^{s,l}\}$ .
2. For each  $s, l$ :  $\{D_m^{s,l} | m = 0 \dots M-1\}$ .

### 4.3 Translation Using Sorter

An  $n$ -bit Boolean sorter is an  $n$ -input  $n$ -output Boolean function  $\langle y_1, \dots, y_n \rangle = \text{Sort}(x_1, \dots, x_n)$  satisfying the following constraints:

1. If  $y_i = 1$ , then  $y_j = 1$  for all  $j \leq i$ ,
2. The number of *true* input variables is the same as the number of *true* output variables, i.e.,  $|\{i : x_i = \top\}| = |\{i : y_i = \top\}|$ .

In unary representation, the numerical value of a bit-vector is the number of bits set to *true*. Bit-vector  $V_i = \langle x_i, \dots, x_i \rangle$ , where  $|V_i| = a_i$  represents either 0 or  $a_i$ , depending on the value of  $x_i$ . It is straightforward to see that  $\sum a_i x_i = m$  is equisatisfiable with the conjunction of the following three conditions:

1.  $\langle y_1, \dots, y_S \rangle = \text{Sort}(V)$ , where  $V = \langle x_1, \dots, x_1, x_2, \dots, x_2, \dots, x_n, \dots, x_n \rangle$  is a bit vector and each  $x_i$  occurs  $a_i$  times in  $V$  and  $S = \sum a_i$ ,
2.  $y_m = \text{true}$ ,
3.  $y_{m+1} = \text{false}$ .

The above construction can be used to generate a valid translation for a given PMod-constraint. Let  $C_{\text{Sorter}}$  be the set of clauses describing the relation between input variables  $V$ , output variables  $Y = \langle y_1, \dots, y_n \rangle$  and auxiliary variables for a sorter. Then, pair  $\langle v, C \rangle$  is a valid translation for (5) where  $C = C_{\text{Sorter}} \cup C_v$ , and  $C_v$  is the set of clauses describing

$$v \Leftrightarrow \bigvee_{j \equiv b' \bmod M} y_j$$

A sorter network can be constructed either a sorting network, or BDD encoding.

**Proposition 8** *Let  $C_{Sorter}$  be the set of clauses describing a sorter and  $C_v$  be the set of clauses describing  $v \Leftrightarrow \bigvee_{j \equiv b' \pmod M} y_j$ . Then, the pair  $\langle v, C \cup C_{Sorter} \rangle$  is a valid translation for (5).*

#### 4.4 Translation Using Cardinality Constraints

Let a cardinality constraint be as what we have described in constraint on a set of Boolean variables which restricts the number of True variables in the set. It can be seen that a cardinality constraint is a special case of PB-constraints where all coefficients are one:

$$C : x_1 + \dots + x_n = b. \quad (6)$$

Essentially, (6) asserts that a satisfying assignment for  $C$  should map exactly  $b$  literals out of the literals in set  $\{x_1, \dots, x_n\}$  to *true*. There are many approaches to produce a valid translation for a cardinality constraint, see [1].

Having a PBMod-constraint in form (5), it can be rewritten as the following constraint:

$$\sum_{i=0}^{M-1} \#(\{x_j \mid a_j \pmod M = i\}) * i \equiv b' \pmod M, \quad (7)$$

where  $\#(\{y_1, \dots, y_m\})$  represents the number of literals mapped to *true*.

**Proposition 9** *Unit-propagation infers inconsistency in the generated CNF of BDD translation iff the PBMod-constraint is unsatisfiable. UP infers the value of an input variable,  $x_i$ , iff that variable takes a unique value in all solutions of the input PBMod-constraint. If the PBMod-constraint has exactly one solution, UP is able to infer all input variables values.*

The proof of Proposition (9) is essentially the same as the proof for arc consistency of BDD encoding.

**Theorem 2** *Using BDD encoding as the translation oracle in Theorem 1, one can translate the PB-constraint  $Q : \sum a_i l_i = b$  into a CNF with  $n \sum P_i \leq nmP_m \leq n \log S \log S \leq n(\log n + \log a_{Max})^2$  variables,  $O(n(\log n + \log a_{Max})^2)$  clauses and  $O(n(\log n + \log a_{Max})^2)$  literals.*

Until now, we described how a PB-constraint can be translated into a series of PBMod-constraint and how a PBMod-constraint can be translated into CNF. In example 2, we demonstrate the procedure of converting a PB-constraint to CNF.

**Example 2** *Consider the following PB-constraint. For this case, we have  $S = 15$  and  $P = \{2, 3, 5\}$ .*

$$1x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 = 7$$

Let  $\langle v_2, C_2 \rangle$ ,  $\langle v_3, C_3 \rangle$  and  $\langle v_5, C_5 \rangle$  be valid translations for the following PBMod-constraints, respectively:

$$1x_1 + 0x_2 + 1x_3 + 0x_4 + 1x_5 = 1(\text{mod } 2)$$

$$1x_1 + 2x_2 + 0x_3 + 1x_4 + 2x_5 = 1(\text{mod } 3)$$

$$1x_1 + 2x_2 + 3x_3 + 4x_4 + 0x_5 = 2(\text{mod } 5)$$

Then,  $\langle v, C_2 \cup C_3 \cup C_5 \cup C' \rangle$ , where  $v$  is a new variable and  $C'$  is the set of clauses necessary to describe  $v \Leftrightarrow v_2 \wedge v_3 \wedge v_5$ .

Note that every encodings for PB-constraints can directly be converted to an encoding for PBMod-constraints using the following observation:

$$\sum a_i l_i = b(\text{mod } M) \Leftrightarrow \exists k \ 0 \leq k \leq \text{Max} : \sum a_i l_i = b + k * M$$

where  $\text{Max} = \lfloor \frac{\sum a_i}{M} \rfloor < \lfloor \frac{n*(M-1)}{M} \rfloor < n$  as the left-hand side is an integer in range  $[0 \cdots \sum a_i]$ .

We know that every integer in range  $[0 \cdots \text{Max}]$  can be encoded using  $\log(\text{Max} + 1)$ -bits. So, the following two constraints are equivalent, i.e., every solution to one of them can be uniquely converted to a solution to another one.

$$\sum a_i l_i = b(\text{mod } M) \tag{8}$$

$$\sum a_i l_i - 1k_0 - 2^1 k_1 - \dots - 2^{\lfloor \log(\text{Max}+1) \rfloor} k_{\lfloor \log(\text{Max}+1) \rfloor} = b \tag{9}$$

So, instead of encoding PBMod-constraint 8, one can encode the normalized version of PB-constraint 9 using any encoding which produces a valid translation for PB-constraints.

In particular, if we use the *Totalizer based* encoding, [5], in the above approach, we get an encoding encoding for PBMod-constraints whose CNF has at most  $n^4 \log n \log M$  clauses,  $n^3 \log n \log M$  auxiliary variables and  $n^4 \log n \log A$  literals. And then, we will have an encoding for PB-constraints which produces a CNF with  $n^4 \log n * (\log n + \log a_{\text{Max}})$  clauses,  $n^3 \log n * (\log n + \log a_{\text{Max}})$  auxiliary variables and  $n^4 \log n (\log n + \log a_{\text{Max}})$  literals. But the resulting encoding for PBMod-constraints will not be arc consistent, because as we show in the next section, totalizer based encoding is not arc-consistent, for certain PB-constraints.

## 5 Previous Work

The existence of a polynomial size arc-consistent encoding for PB-consistent in form  $\sum a_i x_i < b$  was an open question until very recently. Bailluex et al. developed an arc-consistent polynomial size translation for these constraints [5]. Although all kinds of PB-constraints can be written as conjunction of at most two constraints in the form  $\sum a_i l_i < b$ , arc-consistency is not preserved for PB-constraints in the form  $\sum a_i l_i = b$ . Moreover, in section 6, we prove there cannot be a polynomial size arc-consistent encoding for all possible PB-constraints in form  $\sum a_i l_i = b$  unless  $P = \text{CoNP}$ .

## 5.1 Arc-consistent Encodings

**Translation through BDD** This approach is similar to the dynamic programming solution for solving the subset-sum problem. For every possible pair  $i$  and  $j$  where  $0 \leq i \leq n$ ,  $0 \leq j \leq b$ , a fresh Tseitin variable is introduced,  $D_j^i$ , and using appropriate clauses the relation between  $D_j^i$ ,  $x_i$ ,  $D_j^{i-1}$  and  $D_{j-a_i}^{i-1}$  are described.

$$D_i^j = \begin{cases} \top & \text{if } i \text{ and } j \text{ are both zero;} \\ \perp & i = 0 \text{ and } j > 0; \\ (D_{j-a_i}^{i-1} \wedge x_i) \vee (D_j^{i-1} \wedge \neg x_i) & \text{Otherwise} \end{cases}$$

Describing  $D_j^i$  variables in a top-down manner, as proposed by [4], usually generate fewer number of Tseitin variables and smaller CNF than the bottom-up procedure. Translation through BDD is generalized arc-consistent but it might produce an exponential size CNF with respect to the input size.

## 5.2 Non-Arc-consistent Encodings

**Binary Encoding (Bin)** Every circuit can be translated into CNF, and so the binary adders can be described using a series of clauses. The main idea in this approach is to use binary encoding of integers and using the fact that setting  $x_i$  to false is the same as setting  $a_i$  to zero. Every coefficient in a PB-constraint,  $a_i$ , is represented as a vector of bits  $\langle c_i^1 \wedge x_i, \dots, c_i^k \wedge x_i \rangle$  and each of these vectors is fed into an adder-network. The output of the adder-network is compared with the binary representation of  $b$ .

The size of CNF generated using this encoding is polynomial with respect to the size of input but unit propagation performs poorly on the produced CNF.

**Translation Through Totalizer** In [5], the authors described an encoding for PB-constraints in form  $Q : \sum a_i x_i < b$  which fully supports generalized arc-consistency and produces a polynomial size CNF. In their context, setting a variable from  $X$  to false never makes the constraint inconsistent, i.e., the formula  $\neg Q$  is a *monotone formula* [2].

They used gadgets, called *polynomial watchdog*. A polynomial watchdog associated with the constraint  $Q$  on variables  $X$  is a CNF formula,  $PW(Q)$ , such that for every partial assignment to the input variables,  $X$ , that violates the constraint  $Q$ , unit propagation applied to  $PW(Q)$  infers the value *true* for the output variable of  $PW(Q)$ .

If constraint  $Q : \sum a_i x_i < b$  is not satisfiable under a partial assignment, the sum of coefficients of variables which are set to true under the current partial assignment should be greater than or equal to  $b$ . The variable  $x_k$  is forced to be false under current assignment iff  $Q_k : \sum_{i \neq k} a_i x_i < b - a_k$ , is not consistent. Global polynomial watchdog, GPW, and Local polynomial watchdogs, LPW, are used to enable UP to do these kinds of inferences. The following can be used as an encoding for PB-constraint  $Q$ :

$$F = \neg GPW(Q) \wedge \bigwedge LPW(Q_k) \Rightarrow (\neg x_k).$$

Having access to an encoding for PB-constraints in the form  $Q : \sum a'_i l_i < b'$ , one can build an encoding for constraint  $Q' : \sum a_i l_i = b$  using the following observation:

**Observation 4** *The set of solutions to (1) is the same as the intersection of sets of solutions to (2) and (3)*

1.  $\sum a_i l_i = b$
2.  $\sum a_i l_i < b + 1$
3.  $\sum a_i \neg l_i < \sum a_i + 1 - b$

There are normalized PB-constraints for which totalizer based translation is not arc-consistent but our encoding is. We characterized these instances in section 6.

**Translation Through Network of Sorters (SN)** A sorting network is a circuit with  $n$  input wires and  $n$  output wires consisting of a set of comparators with two input wires and two output wires. Each output of a comparator is used as an input to another comparator except those used as output wires of the sorting network.

In this translation, a mixed-base,  $B = \langle B_1, \dots, B_k \rangle$  is selected. And each coefficient,  $a_i$ , is represented using a vector of size  $k$ ,  $\langle c_i^1, \dots, c_i^k \rangle$  such that  $0 \leq c_i^j < B_j$  and

$$a_i = \sum_{j=1}^k c_i^j \prod_{k=1}^{j-1} B_k$$

Then each digit,  $c_i^j$ , is represented using  $B_j$  bits (in unary encoding).  $k$  sorting networks are used to implement an adder-circuit which computes the summation of  $(a_i \wedge x_i)$  for  $i = 1 \dots n$ . One can find more details about the translation using a network of sorters in [7].

The size of the CNF generated using this encoding is polynomial with respect to the size of input. This encoding is arc-consistent if all the coefficients are one. This special class of PB-constraints is called *Cardinality Constraint* in SAT community. There are some well-known encodings for cardinality constraints which are arc-consistent and produce smaller CNFs [1].

### 5.3 Summary

Table 1 summarizes the number of auxiliary variables, clauses, and literals produced by each approach in the translation of  $a_1 l_1 + \dots + a_n l_n = b$ .

BDD encoding is the only encoding which is generalized arc-consistent for this kind of PB-constraint. This encoding may produce exponential size CNF.

We show in section 6 that Totalizer encoding is not arc-consistent for all constraints whose comparison operator is ‘=’. The translation using sorting networks has a reasonable size but it is arc-consistent if all the coefficients are equal to one (The authors in [7] demonstrated a *necessary condition* for arc-consistency). Our encoding, equipped with  $\mathbb{M}^p$  as the set of modulus and BDD translation for PMod-constraints as translation oracle, produces a polynomial size CNF. In the next section, we show that the number of instances for which the CNF obtained by the proposed encoding is generalized arc-consistent is much more than that of sorting networks. And there are many instances for which our encoding is arc-consistent while totalizer-based encoding is not.

**Table 1.** Performance of Translations ( $a_{Max} = \text{Max}\{a_i\}$ )

	# of Auxiliary Vars.	# of Clauses	Size of CNF
BDD	$O(n^2 a_{Max})$	$O(n^2 a_{Max})$	$O(nb)$
Totalizer	$O(n^2 \log n \log a_{Max})$	$O(n^3 \log n \log a_{Max})$	$O(n^3 \log n \log a_{Max})$
Bin	$O(n \log a_{Max})$	$O(n \log a_{Max})$	$O(n \log a_{Max})$
SN	$O(n \log a_{Max} \log^2 \log a_{Max})$	$O(n \log a_{Max} \log^2 \log a_{Max})$	$O(n \log a_{Max} \log^2 a_{Max})$
Proposed	$O(n(\log n + \log a_{Max})^2)$	$O(n(\log n + \log a_{Max})^2)$	$O(n(\log n + \log a_{Max})^2)$

In summary, Totalizer-based encoding, Sorting Network encoding and our encoding produce polynomial size translations for PB-constraint in form  $\sum a_i l_i = b$  and each of them is arc-consistent for a certain subset of all possible PB-constraints.

## 6 Performance of Unit Propagation

In this section, we show that there cannot be an encoding for PB-constraint in form  $\sum a_i l_i = b$  which always produces a polynomial size arc-consistent CNF. Also we study the arc-consistency of our encoding as well as that of Sorting Network and Totalizer encodings.

### 6.1 Hardness Result

Here, we show that it is not very likely to have an arc-consistent encoding which always produces polynomial size CNF.

**Theorem 3** *There does not exist a UP-detectable encoding which always produces polynomial size CNF unless  $P = \text{CONP}$ . There does not exist a UP-maintainable encoding which always produces polynomial size CNF unless  $P = \text{CoNP}$ .*

**Proof** Unit propagation, on a set of clauses, completes its execution either by reporting inconsistency or eliminating some variables from the input CNF. The

worst-case running time of unit propagation is polynomial in size of the input CNF.

The subset sum problem is: given a set of integers  $A = \{a_1, \dots, a_n\}$  and an integer  $b$ , does the sum of a non-empty subset equal to  $b$ ? This problem can be represented as the following PB-constraint:

$$Q : a_1x_1 + \dots + a_nx_n = b$$

We know that the subset sum problem is an NP-complete problem. Now, assume there exists an encoding whose resulting CNF is UP-detectable for all PB-constraints in the form  $\sum a_i l_i = b$ . Let's call this encoding  $E$ . Based on definition of UP-detectability,  $E$  gets a PB-constraint  $Q$  and returns a valid translation  $\langle v, C \rangle$  such that

$$Q \models \perp \Leftrightarrow v \wedge C \Big|_{UP} \perp.$$

The formula  $Q \models \perp$  asserts that  $Q$  is not satisfiable, i.e., the original subset sum problem does not have any solution. The fact that UP can infer inconsistency on  $v \wedge C$  in polynomial time with respect to the number of literals in  $\{v\} \cup C$  implies that if  $C$  has polynomial size, with respect to  $Q$ , deciding if the answer to a subset sum instance is 'No' is easy. That is, either there are PB-constraints whose corresponding CNFs are not polynomial size or  $\text{CoNP}=\text{P}$ .

Now, consider the following problem: Given a normalized PB-constraint  $Q : \sum a_i l_i = b$ , does it have exactly one solution?

The Unique SAT problem, USAT, can be reduced to this problem. The reduction is similar to the reduction explained in [13] to prove the NP-hardness of subset sum problem (we did not include it in this paper for sake of space). It is already known that USAT belongs to complexity class  $D^P$  and it is  $\text{CoNP}$ -hard [11].

Let  $Q : \sum a_i x_i = b$  be the output of the reduction on the USAT instance  $C$ .  $C$  has exactly one solution iff  $Q$  has exactly one solution. But if  $Q$  has exactly one solution,  $\mathcal{A}$ , we have  $Q \models x_i$  iff  $\mathcal{A} \models x_i$  and  $Q \models \neg x_i$  iff  $\mathcal{A} \not\models x_i$ . Let  $\langle v, C \rangle$  be a UP-inferable translation for  $Q$ , then we should have

$$\forall i : \mathcal{A} \models x_i : C \wedge v \Big|_{UP} x_i \quad \forall i : \mathcal{A} \not\models x_i : C \wedge v \Big|_{UP} \neg x_i \quad (10)$$

So, UP can infer all input variables values,  $x_1, \dots, x_n$ , when it is executed on  $C \wedge v$  iff the given subset sum instance has exactly one solution.

Throughout the rest of this section, we assume we are given a PB-constraint,  $Q : \sum a_i l_i = b$  and a valid translation for it,  $\langle v, C \rangle$ . Also, let  $Q_1, \dots, Q_m$  be the PBMod-constraints generated during the translation process and  $\langle v_i, C_i \rangle$  be a valid translation for  $Q_i$ . Also, assume  $Ans = \{A_1, \dots, A_r\}$  is the set of all possible solutions to  $Q$ .

## 6.2 Arc-consistency for Proposed Encoding

There are three situations in which UP is able to infer the input variables values and so one can expect SAT solvers to perform well in those situations:

1. **Unit Propagation Detects Inconsistency:** One can infer there is no assignment satisfying  $Q$  by knowing  $Ans = \emptyset$ . We call the unsatisfiable constraints whose translations are UP-detectable to be *good constraints*.  
UP gets  $\{v\} \cup C$  as its input, it detects  $v$  should be true and next, it finds out  $v_i$  is true, for all  $1 \leq i \leq m$ . Based on Proposition 9, if at least one of the  $m$  PMod-constraints is unsatisfiable, UP detects inconsistency.
2. **Unit Propagation Solves Constraint:** One can infer the solution for  $Q$  if there is just a single satisfying solution to  $Q$ , i.e.,  $Ans = \{A_1\}$ . For this kind of constraints, UP might be able to infer the correct values for all input variables ( $X$ ). We call the constraints which have exactly one solution and UP is able to solve them completely the *nice constraints*. Note that after a consistent solution to the input variables has been found, the values of all auxiliary variables generated during the translation are either forced or ‘don’t care’.  
UP gets  $\{v\} \cup C$  as its input, it detects  $v$  should be true and next, it finds out  $v_i$  is true, for all  $1 \leq i \leq m$ . Based on Proposition 9, if at least one of the  $m$  PMod-constraints has exactly one solution, UP is able to infer all the input variables value.
3. **Unit Propagation Infers the Value for an Input Variable:** One can infer the value of input variable  $x_k$  is *true/false* if  $x_k$  takes the same value in all the solutions to  $Q$ . For this kind of constraints, UP might be able to infer the value of  $x_k$ . Note that the nice constraints are a subset of these constraints. Similar to case of nice constraints, UP detects  $v$  should be true and next, it finds out  $v_i$  is true, for all  $1 \leq i \leq m$ . Based on Proposition 9, UP infers the correct value for  $x_k$  if  $x_k$  has the same value in all of solutions to at least one of the  $m$  PMod-constraints.

These three cases are illustrated in the following example.

**Example 3** *In this example, we use the same PB-constraint as we used in Example 2.*

1. *If  $A$ , the current partial assignment, is  $A = \{\neg x_2, \neg x_4\}$  and  $P = 5$ . There is no total assignment satisfying  $1x_1 + 3x_3 = 2$ .*
2. *If  $A$ , the current partial assignment, is  $A = \{x_2, \neg x_3, x_5\}$  and  $P = 3$ , there is exactly one total assignment ( $\{\neg x_1, x_2, \neg x_3, \neg x_4, x_5\}$ ) which extends  $A$  and satisfies the PMod-constraint.*
3. *If  $A$ , the current partial assignment, is  $A = \{\neg x_3, \neg x_5\}$  and  $P = 2$ , there are four total assignments extending  $A$  and satisfying the PMod-constraint. In all of them,  $x_1$  is in the solution.*

In the rest of this section, we estimate the number of good and nice constraints, i.e., we give a lower bound for the number of constraints whose translation can be solved just by using unit propagation.

Let us assume the constraints are selected, uniformly at random, from  $\{\sum a_1 l_1 + \dots + a_n l_n = b : 1 \leq a_i \leq A = 2^{R(n)} \text{ and } 1 \leq b \leq n * A\}$  where  $R(n)$  is a polynomial in  $n$  and  $R(n) > n$ . To simplify the analysis, we use the same prime modulus  $\mathbb{M}^P = \{P_1 = 2, \dots, P_m = \theta(R(n)) > 2n\}$  for all possible constraints.

Consider the following PMod-constraints:

$$1x_1 + \cdots + 1x_{n-1} + 1x_n = n + 1 \pmod{P_m}, \quad (11)$$

$$1x_1 + \cdots + 1x_{n-1} + 2x_n = n + 1 \pmod{P_m}, \quad (12)$$

$$1x_1 + \cdots + 1x_{n-1} + nx_n = 2n - 2 \pmod{P_m}. \quad (13)$$

One can verify that (11) does not have any solution, (12) has exactly one solution and  $x_n$  is *true* in all solutions for (13). *Chinese Remainder Theorem*, [6], implies that there are  $(A/P_m)^{n+1} = 2^{(n+1)Q(n)}/Q(n)^{n+1}$  different PB-constraints in the form  $\sum a_i l_i = b$  such that their corresponding PMod-constraints, where the modulo is  $P_m$ , are the same as (11). The same thing is true for (12) and (13).

### 6.3 UP for Sorting Network

Here, we show that there are more instances for which our encoding maintains arc-consistency than Sorting Network.

It is stated in [7]: “Unfortunately, arc-consistency is broken by the duplication of inputs, both to the same sorter and between sorters.”

As we described in Section 5, in Sorting Network encoding, one fixes a multi-base  $B = \langle B_1, \dots, B_m \rangle$ . To avoid duplication between sorters, each coefficients,  $a_i$ , should have a single non-zero digit in their multi-base  $B$ -representation. To avoid duplication in the same sorter, the non-zero digit should be exactly 1. So, each coefficient can take  $m$  different values, based on the position of its non-zero digit. There are  $n$  coefficients, so there are at most  $nAm^n$  different instances which are arc-consistent, where  $nA$  is the maximum number of possible right-hand side of the equation. Having  $B_i \geq 2$  implies that  $m \leq \log A$ .

### 6.4 UP for Totalizer-based Encoding

In [5], it is claimed that, totalizer-based encoding is a polynomial size CNF encoding such that generalized arc-consistency is maintained through unit propagation for all PB-constraints in the following form:

$$\sum a_i l_i \{=, >, \geq, <, \leq\} b.$$

Although totalizer-based encoding is generalized arc-consistent for the PB-constraints in the forms  $\sum a_i l_i \{>, \geq, <, \leq\}$ , it does not produce an arc-consistent translation for some PB-constraints in the form  $\sum a_i l_i = b$ .

In their approach, the PB-constraint  $Q : \sum a_i l_i = b$  should be converted to the following two constraints:

$$\sum a_i l_i < b + 1, \quad \sum a_i \neg l_i < \sum a_i + 1 - b. \quad (14)$$

Consider the following PB-constraint:

$$Q_1 : 3x_1 + 3x_2 + 4x_3 = 7,$$

As  $Q_1(3) : 0x_1 + 0x_2 + 1x_3 = 1$ , UP, and also our approach, can infer that  $x_3$  should be true. Now consider the following two constraints:

$$Q_2 : 3x_1 + 3x_2 + 4x_3 < 8,$$

$$Q_3 : 3\neg x_1 + 3\neg x_2 + 4\neg x_3 < 10 - 6 = 4.$$

Let  $\langle v_2, C_2 \rangle$  and  $\langle v_3, C_3 \rangle$  be valid translations obtained from totalizer-based encoding for  $Q_2$  and  $Q_3$ , respectively. UP does not infer anything from  $v_2 \wedge C_2$  because nothing can be inferred about any of  $x_i$ s by knowing  $Q_2$  should be true. We have the same situation for  $Q_3$ .

In fact, the translation produced by totalizer-based encoding is not generalized arc-consistent for almost all PB-constraints which have a PBMod-constraint in form (11) or (10).

We summarize the discussion above in the following observations:

**Observation 5** *There are at most  $(\log A)^n$  instances where the CNF produced by Sorting Network encoding maintains arc-consistency, while this number for our encoding is at least  $(A/\log(A))^n$ . So, if  $A = 2^{R(n)}$ , almost always we have  $2^{R(n)}/R(n) \gg R(n)$ .*

**Observation 6** *There is a family of PB-constraints whose translation through totalizer-based encoding is not arc-consistent but the translation obtained by our encoding is arc-consistent.*

## 7 Conclusion and Future Work

We presented a method for translating Pseudo-Boolean constraints into CNF. The size of produces CNF is polynomial with respect to the input size. We also showed that for exponentially many instances, the produced CNF is arc-consistent. This number is much bigger than that of the existing encodings.

The upper bounds on the size of CNF are not tight. One needs to analyze the performance of the proposed method more carefully and find a tighter bounds on the CNF size. We still need to implement the proposed encoding and compare it with the other encodings on some real-life problems.

## References

1. A. Aavani, N. Wu, D. Mitchell, and E. Ternovska. Grounding Count Aggregates. *Logic for Programming Artificial Intelligence and Reasoning*, 2010.
2. N. Alon and R.B. Boppana. The monotone circuit complexity of Boolean functions. *Combinatorica*, 7(1):1–22, 1987.
3. F.A. Aloul, A. Ramani, I. Markov, and K. Sakallah. PBS: a backtrack-search pseudo-boolean solver and optimizer. In *Proceedings of the 5th International Symposium on Theory and Applications of Satisfiability*, pages 346–353. Citeseer, 2002.
4. O. Bailleux, Y. Boufkhad, and O. Roussel. A translation of pseudo Boolean constraints to SAT. *Journal on Satisfiability, Boolean Modeling and Computation*, 2:191–200, 2006.

5. O. Bailleux, Y. Boufkhad, and O. Roussel. New Encodings of Pseudo-Boolean Constraints into CNF. *Theory and Applications of Satisfiability Testing-SAT 2009*, pages 181–194, 2009.
6. C. Ding, D. Pei, and A. Salomaa. *Chinese remainder theorem: applications in computing, coding, cryptography*. World Scientific Publishing Co., Inc. River Edge, NJ, USA, 1996.
7. N. Eén and N. Sorensson. Translating pseudo-boolean constraints into SAT. *Journal on Satisfiability, Boolean Modeling and Computation*, 2(3-4):1–25, 2006.
8. B. Farhi and D. Kane. New results on the least common multiple of consecutive integers. In *Proc. Amer. Math. Soc*, volume 137, pages 1933–1939, 2009.
9. G.H. Hardy, E.M. Wright, D.R. Heath-Brown, and J.H. Silverman. *An introduction to the theory of numbers*, volume 6. Clarendon press Oxford, 1979.
10. RV Kulkarni and PR Bhawe. Integer programming formulations of vehicle routing problems. *European Journal of Operational Research*, 20(1):58–67, 1985.
11. C.H. Papadimitriou and M. Yannakakis. The complexity of facets (and some facets of complexity). In *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pages 255–260. ACM, 1982.
12. H.M. Sheini and K.A. Sakallah. Pueblo: A hybrid pseudo-boolean SAT solver. *Journal on Satisfiability, Boolean Modeling and Computation*, 2:61–96, 2006.
13. M. Sipser. *Introduction to the Theory of Computation*. International Thomson Publishing, 1996.
14. G.S. Tseitin. On the complexity of derivation in propositional calculus. *Studies in constructive mathematics and mathematical logic*, 2(115-125):10–13, 1968.

## A Proposition 7 (Proof)

Here, we prove Proposition (1) presented in section 3.

Let  $\mathbb{M}^P$  be the set of  $m$  first prime numbers,  $\mathbb{M}^P = \{2, 3, \dots, P_m\}$  and  $S$  be an integer.

Prime number theorem, [9], states that the number of prime number less than or equal to an integer  $x$ ,  $\pi(x)$ , satisfies the following:

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln(x)} = 1. \quad (15)$$

Using (15), we can bound the value of  $\prod_{p \in \mathbb{M}^P} p$ , by:

$$\left(\frac{P_m}{e}\right)^{\pi(P_m) - \pi(P_m/e)} \leq \prod_{p \in \mathbb{M}^P} p \leq (P_m)^{\pi(P_m)} \quad (16)$$

By setting  $\pi(x) = x/\ln x$ , we can rewrite (16) as:

$$\left(\frac{P_m}{e}\right)^{P_m/\ln(P_m) - P_m/(e*\ln(P_m/e))} \leq \prod_{p \in \mathbb{M}^P} p \leq (P_m)^{P_m/\ln(P_m)} \leq e^{P_m} \quad (17)$$

A lower bound for  $\prod_{p \in \mathbb{M}^P}$  can be obtained as follows:

$$\begin{aligned}
& \left( \frac{P_m}{e} \right)^{P_m / \ln(P_m) - P_m / (e * \ln(P_m / e))} \\
&= (e)^{\frac{P_m * (\ln P_m - 1)}{\ln P_m} - \frac{P_m}{e}} \geq (e)^{\frac{P_m}{2} - \frac{P_m}{e}}
\end{aligned} \tag{18}$$

From (17) and (18):

$$(e)^{\frac{P_m}{2} - \frac{P_m}{e}} \leq \prod_{p \in \mathbb{M}^p} p \leq e^{P_m} \tag{19}$$

$$\prod_{p \in \mathbb{M}^p} p \in e^{\theta(P_m)} \tag{20}$$

The last equation, (20), states that the maximum value in  $\mathbb{M}^p$  whose product is larger than a given  $S$  is  $\theta(\ln S)$ .

Now, by applying the prime number theorem once more, we get that:

$$m = |\mathbb{M}^p| \approx \frac{P_m}{\ln P_m} = \theta\left(\frac{\ln S}{\ln \ln S}\right)$$